Análisis e Implementación de Sistema de Detección de Amenazas Distribuido Basado en Deep Learning

Felipe Pinto Guzmán

Abstract— **Durante la última década se ha experimentado un crecimiento significativo en el número de dispositivos inteligentes, los cuales son capaces de conectarse a la internet para comunicarse entre sí conformando la Internet de las Cosas. Sin embargo, junto a las ventajas que brinda esta nueva tecnología aparecen nuevas posibles amenazas en cuanto a cyber-seguridad que requieren el uso de nuevas técnicas al momento de enfrentarlas dada las diferencias en la arquitectura de este nuevo tipo de redes con respecto a la Internet clásica. Razón por la que en este trabajo se propone implementar y probar un enfoque basado en Deep Learning para abordar estas amenazas.**

I. INTRODUCCIÓN

Siendo una tecnología emergente, Ïnternet de las Cosas"ha abierto nuevos horizontes en cuanto al desarrollo de ciudades inteligentes. Estas se cimientan en la capacidad de recolección, procesamiento y comunicación de datos que ofrecen las distintas aplicaciones implementadas en cada dispositivo inteligente.

Específicamente, el poder comunicar grandes cantidades de datos a través de la Internet, junto a las ventajas que ofrece, también conlleva potenciales peligros relacionados a potenciales amenazas provenientes del cyber-crimen. Donde estos ya no se limitan solo al ámbito virtual, sino que tienen la capacidad de actuar directamente sobre el mundo físico mediante los distintos dispositivos, de forma que representa un peligro mayor para la población en general.

El objetivo de este trabajo se centra en analizar el tráfico que circula a través de la estructura una red orientada a Ïnternet de Las Cosas", cuyos requerimientos de baja latencia, limitación de recursos, escalabilidad y movilidad no pueden ser satisfechos a cabalidad por una red centralizada [3]. En torno a este objetivo se realiza una caracterización de la arquitectura de red tipo "Fog Network"[2], la cual se conforma de redes altamente distribuidas y heterogéneas. Razón por la que distintas técnicas utilizadas para detectar ataques en la nube no funcionan al momento de ser aplicados en este escenario.

Principalmente, la detección de amenazas puede ser basada en firma o en identificación de anomalías. El enfoque por firma compara el tráfico entrante con datos de ataques conocidos previamente mientras que el por detección de anomalías busca desviaciones con respecto al tráfico normal. El primero ha sido ampliamente utilizado, pero a su vez también criticado por su falta de precisión al momento de detectar nuevos ataques. Por otra parte, el segundo sí es capaz de cumplir con este requisito, sin embargo, también presenta un gran porcentaje de falsos positivos. Para la implementación de ambos enfoques se han utilizado algoritmos clásicos de aprendizaje de máquinas, pero estos se han visto sobrepasados frente a la creciente complejidad de las amenazas.

Una característica importante de los distintos cyber-ataques perpetrados es su dependencia lógica con respecto a versiones anteriores, pudiendo representar desde una pequeña mutación hasta algo talmente nuevo, sin embargo en este ultimo caso generalmente se mantiene una estructura abstracta que lo relaciona con amenazas ya conocidas. Por esta razón, se cree que algoritmos basados en el uso de "Deep Learningçonforman una opción viable para abordar el problema dada su capacidad de llevar a cabo la identificación de estas características internas.

II. TRABAJOS RELACIONADOS

A la fecha existen diversas aproximaciones a este problema utilizando "Deep Learning.ªsí como la creación de distintos datasets que reflejan distintos tipos de ataques perpetrados a través de la red mediante diversas capas y protocolos de estas.

Una de las primeras implementaciones de este enfoque viene dada por [4] que utiliza aprendizaje no supervisado para obtener las características más indicativas mediante el uso de un auto encoder. Luego, estas son probadas frente a un dataset etiquetado para decidir si representan un ataque o tráfico normal. Sin embargo, en este caso los autores consideran una arquitectura de red centralizada, es decir, se utiliza un modelo único para analizar al tráfico de toda la red. Mientras que el objetivo del trabajo actual es portar estos algoritmos para que sean viables en redes distribuidas, donde es necesario procesar la información en distintos nodos de esta.

Otro trabajo relevante consiste en la aplicación de auto-encoders para detección de anomalías [5], donde el comportamiento normal de la red fue aprendido mediante autoencoders que utilizando no linealidades realizan una reducción del espacio de características a las mas relevantes. En su estudio, los autores demuestran que en el dataset de prueba los registros de tráfico normal tienen un pequeño error al reconstruir la respuesta mientras que en los casos anómalos este aumenta considerablemente.

Otros autores se enfocan la detección de intrusiones a vehículos inteligentes [6]. En este caso se demuestra que el uso de "Deep Belief Networks.[en] el pre procesamiento, que representan un tipo de aprendizaje no supervisado puede mejorar la precisión en la detección de estas. Sin embargo, la aplicación se centra en un nodo especifico de la red por

lo que su enfoque es centralizado y podría no funcionar bien en una ”Fog Network”

III. ANÁLISIS DE CYBER-SEGURIDAD EN IOT

En los últimos años el número de dispositivos conectados a la red ha aumentado exponencialmente donde en las llamadas Çiudades Inteligentes”diversas aplicaciones han afectado áreas relacionadas con el manejo de infraestructura pública, como lo es agua, la electricidad, el transporte, etc. De forma una falla de seguridad puede generar pérdidas masivas en dinero así como en vidas humanas.

Por ende, dada la gran variedad de usos para el Internet de las Cosas en distintas áreas, hace que los posibles ataques también sean diversos. Una encuesta reciente [7] muestra que las familia de ataques mas frecuentes en IoT/Fog Networks son del tipo DoS [8] [10]. Esto se debe a que la interconectividad entre dispositivos facilita el camino para que criminales agoten sus recursos. Por otra parte, existen amenazas provenientes de accesos remotos no autorizados al hacer uso de puertas traseras. Luego, en el siguiente apartado se identifican las categorías mas importantes [9].

III-A. Sonda

- Satan- sondear la red por algunas debilidades conocidas.
- IPsweep- hacer ping a varios hots para relevar la IP del objetivo.
- Portsweep- escanear los puertos para descubrir los servicios disponibles en el host.
- Nmap- distintas formas de mapear la red.

III-B. R2L

- Warezclient- descargar software ilegal subido previamente por el atacante.
- Guess_passwd- adivinar la contraseña sobre telnet.
- Warezmaster- subir software ilegal a servidor FTP explotando vulneravilidades en permisos de escritura.
- Imap- acceso ilegal a cuenta de usuario local explotando vulnerabilidades.
- Ftp_write- crear un archivo anónimo .rhost en FTP para obtener autentificación local.
- Multihop- un escenario de varios días donde usuario vulnera un sistema.
- Phf- CGI script que permite ejecutar comandos arbitrarios en una maquina con un servidor web mal configurado.

III-C. U2R

- Buffer_overflow- uso del comando ffbconfig de UNIX para generar
- Rootkit- habilita acceso de administrador,
- Loadmodule- ganar acceso de root en shell al resetear IFS,
- Perl- creat una shell con permisos de root utilizando ataque en perl que cambia Id del usuario a root,

III-D. DoS

- Smurf- llenar de peticiones de respuesta del tipo ICMP.
- Neptune- llenar de SYN en puertos.
- Back- solicitar una URL teniendo muchos ”backslashes”.
- Teardrop- causar un reinicio del sistema o directamente botarlo usando paquetes UDP mal fragmentados.
- Pod- hacer ping con paquetes mal formados causando reinicio o caida del sistema.
- Land- enviar paquetes UDP teniendo la misma direccion de fuente y destino.

IV. ENFOQUE PROPUESTO

Se tiene un conjunto de nodos ”Fog”que son responsables de entrenar y albergar modelos locales asociados a los dispositivos conectados a la red periférica, esto ya que se encuentran mas cerca de las infraestructuras inteligentes soportadas por la Internet de las Cosas. Luego se tiene un nodo central encargado de coordinar cada uno de los subnodos mediante parámetros y también cumple funciones de optimización. Además de de las ventajas relacionadas con autonomía local para detección de ataques usando entrenamiento con datos locales, se obtienen beneficios relacionados con la aceleración de este gracias a la cercanía con respecto a las fuentes de datos. Luego, se forma estructura mostrada en 1.

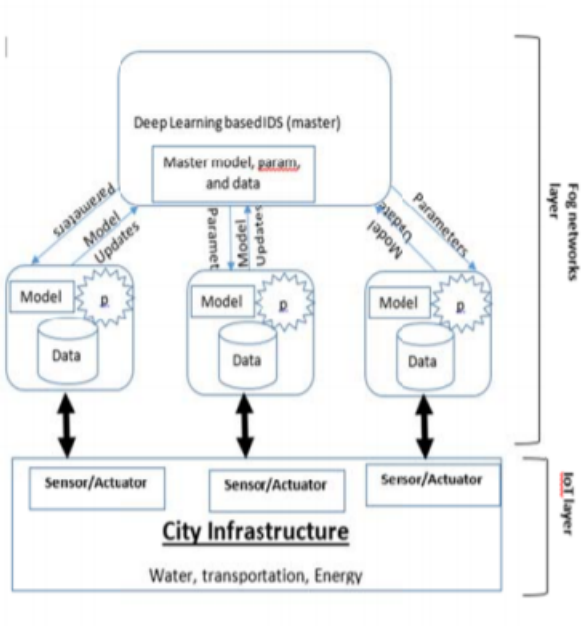

Fig. 1. Arquitectura del modelo de Deep Learning aplicado a una Fog Network. Imagen tomada de [1].

V. IMPLEMENTACIÓN

Se propone implementar la arquitectura propuesta para replicar los resultados obtenidos en [1]. Donde se hace uso del dataset NSL-KDD para obtener información sobre distintos tipos de trafico asociado a diversos protocolos y capas de red.

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	...
0	0.0	b'tcp'	b'ftp_data'	b'SF'	491.0	0.0	b'0'	0.0	0.0	0.0	...
1	0.0	b'udp'	b'other'	b'SF'	146.0	0.0	b'0'	0.0	0.0	0.0	...
2	0.0	b'tcp'	b'private'	b'S0'	0.0	0.0	b'0'	0.0	0.0	0.0	...
3	0.0	b'tcp'	b'http'	b'SF'	232.0	8153.0	b'0'	0.0	0.0	0.0	...
4	0.0	b'tcp'	b'http'	b'SF'	199.0	420.0	b'0'	0.0	0.0	0.0	...

Fig. 2. Descripción del dataset NSL-KDD. Imagen tomada de manuscrito [1].

Luego, se propone clasificar distintos tipos de amenazas mediante etiquetas, utilizando un conjunto de prueba, esto según las categorías mostradas en la imagen 3.

Table 4 (a): traffic distribution of NSL-KDD in 2-class

Traffic	Training	Test
Normal	67343	9711
Attack	58630	12833
Total	**125973**	**22544**

Table 4 (b): traffic distribution of NSL-KDD in multi-class

Traffic	Training	Test
Normal	67343	9711
DoS	45927	7458
Probe	11656	2754
R2L	995	2421
U2R	52	200
Total	**125973**	**22544**

Fig. 3. Imagen tomada de manuscrito [1].

VI. RESULTADOS

Para comparar el rendimiento del algoritmo propuesto, se utiliza como métrica la precisión, dada por el número de verdaderos positivos (detecciones realizadas con éxito) dividido en la cantidad de falsos positivos mas verdaderos positivos. Además, se varía el número de nodos implementados para ver la relación entre este parámetro y el resultado final. En la figura 4 se puede observar el resultado de probar el algoritmo en el conjunto de prueba de la base de datos proporcionada (NSL-KDD DataSeT).

En 4 se observa que efectivamente el modelo distribuido tiene un mejor rendimiento con respecto al centralizado (el cual se basa en la implementación de un solo nodo central). Por otra parte, se nota que el numero de nodos considerados sí aumenta la efectividad del algoritmo, lo cual podría ser beneficioso al momento de considerar su implementación en redes descentralizadas de mayor tamaño.

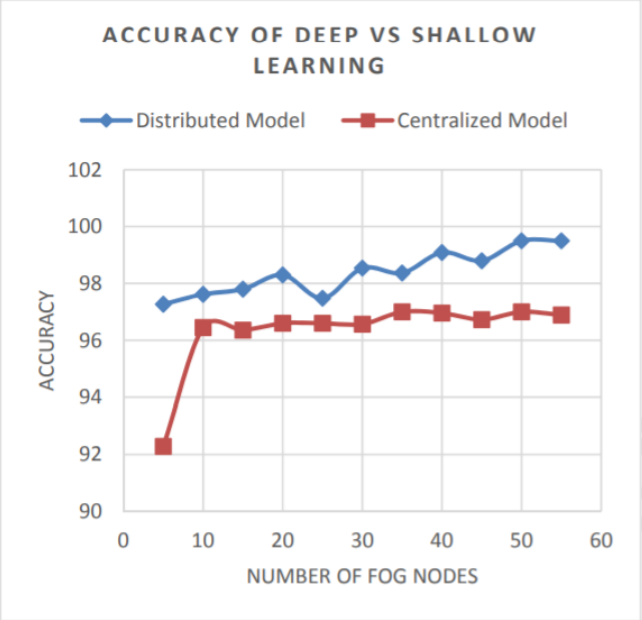

Fig. 4. Gráfica que compara la precisión del modelo propuesto contra la del modelo centralizado. Imagen tomada de manuscrito [1].

Luego, otra variable importante a considerar consiste en el tiempo de entrenamiento asociado a cada algoritmo, es decir, cuanto se demora en converger. En la figura 5 se observa que el modelo distribuido requiere mayor tiempo en comparación con el centralizado, lo que se este debe a que se debe realizar por cada uno de los nodos periféricos en el primer caso. Sin embargo, la diferencia no es grande debido a que se aprovecha la capacidad de paralelización en la red, es decir, entrenar los nodos al mismo tiempo.

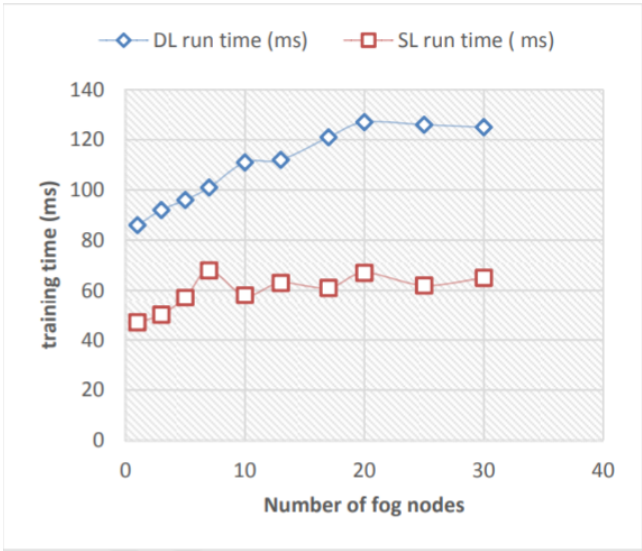

Fig. 5. Gráfica que compara el tiempo de entrenamiento del modelo propuesto contra la del modelo centralizado. Imagen tomada de manuscrito [1].

REFERENCES

[1] Diro, A. A., Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. doi:10.1016/j.future.2017.08.043

[2] Bar-Magen Numhauser, Jonathan (2012). Fog Computing introduction to a New Cloud Evolution. Escrituras silenciadas: paisaje como historiografía. Spain: University of Alcala. pp. 111–126. ISBN 978-84-15595-84-7.

[3] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues,ïn IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, Mar.-Apr. 2017.

[4] Quamar Niyaz, Weiqing Sun, Ahmad Y Javaid, and Mansoor Alam, Deep Learning Approach for Network Intrusion Detection System, ACM 9th EAI International Conference on Bio-inspired Information and Communications Technologies, New York,2016

[5] Sakurada, Mayu, and Takehisa Yairi. .Anomaly detection using autoencoders with nonlinear dimensionality reduction."Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis. ACM, 2014.

[6] Li, Yuancheng, Rong Ma, and Runhai Jiao. .A hybrid malicious code detection method based on deep learning."methods 9.5 (2015).

[7] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," in IEEE Communications Surveys and Tutorials, Vol. 18, No. 1,

[8] Patrikakis, Charalampos, Michalis Masikos, and Olga Zouraraki. "Distributed denial of service attacks."The Internet Protocol Journal 7.4 (2004): 13-35.

[9] @INPROCEEDINGS5356528, author=M. Tavallaee and E. Bagheri and W. Lu and A. A. Ghorbani, booktitle=2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, title=A detailed analysis of the KDD CUP 99 data set, year=2009, volume=, number=, pages=1-6, keywords=security of data;statistical analysis;KDD CUP 99 data set analysis;anomaly detection;signature-based intrusion detection system;attack detection;statistical analysis;Testing;Intrusion detection;Data security;Statistical analysis;Computer security;Computer aided manufacturing;Learning systems;Computational intelligence;Computer networks;Application software, doi=10.1109/CISDA.2009.5356528, ISSN=2329-6267, month=July,

[10] Costa Gondim, João José, et al. .A methodological approach for assessing amplified reflection distributed denial of service on the internet of things."Sensors 16.11 (2016): 1855.